Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1847 12/16/16

~ How Russia Hacked DNC! ~ People Are Talking! ~ "Retro" Battlezone!
~ Yahoo: 1 Billion Hacked ~ Facebook Fact-checking! ~ "Report" Fake News!
~ Nintendo To Support VR! ~ Celebrity Hacker Jailed ~ Scammer Is Charged!

~ Romanians Are Indicted! ~ ~ Popcorn Time Scheme

-* Is Gmail More Secure vs Yahoo *-
-* Yahoo Suffers World's Biggest Hack! *-
-* Facebook Users Are Fed Up With Fake News! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

It's been downright frigid here in the Northeast the past few days! We've also had a little bit of that white stuff, but nothing in the least bit significant; although that could change a lit this weekend. Then again, the forecast is for temps in the low 50's on Sunday, with rain, so a good melting should take care of whatever might fall tomorrow.

It's been another slow week for news, so this week's issue won't be jam-packed with articles. Looking over this issue, it appears that there isn't a whole lot of "positive" articles. Yahoo gets hacked, again. Facebook and fake news is quite dominant. Hackers get caught. Cyber security seems to be a dominant headline these days. Amazing. While technology has done wonders to improve our world and our lives, it's also created a "new" source for severe problems!

As mentioned in recent weeks, we're winding down the days of A-ONE. We've been around for 18 years - longer than Atari itself (at least the company that we remember with fondness!). We've had a lot of fun over the years; and I don't regret [much] putting this endeavor together week after week (with some occasional blips in our publishing schedule). I've enjoyed working with many people working to put A-ONE together, as well as the many people that I have "met" while doing so. I've received countless letters and e-mails over the years - both supportive and critical - whether they pertained to the articles we've published, or the editorial stances/comments that we've made over the years. The fact that you've reacted makes all the difference. And for that, I thank you.

Within the next couple of weeks - before the end of the year - we will publish our last issue. Whether it be next week or the week after will depend on how much material we have available to share with you. Even to the last, I want to be able to have an issue that's filled with news.

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Nintendo’s Next Console Will Support VR?
""""""""""""""""""""""""""""""""" PS4’s Battlezone To Look Like the 1980s Origi
nal!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

It Sure Looks Like Nintendo’s Next Video Game Console Will Support Virtual Reality

Just over 20 years ago, Nintendo released its least successful game console ever: the Virtual Boy. It was a red and black monstrosity with mostly terrible games.

The console was quickly scrapped in favor of more traditional hardware like the Nintendo 64 and GameCube.

But in the past few years, virtual reality has re-emerged as a viable medium. Headsets from Google, Facebook, and Samsung are all commercially available; most notably, Nintendo’s two main competitors, Sony and Microsoft, are making major investments in VR.

Sony’s PlayStation VR headset launched in October it’s powered by the most popular game console in the world, the PlayStation 4.

In 2017, Microsoft is planning to launch a far more powerful Xbox One, currently dubbed "Project Scorpio." That console will be capable of powering high-end VR headsets; the expectation is that Facebook’s Oculus Rift headset will work with Project Scorpio, but nothing specific has been announced just yet.

So that leaves Nintendo.

The company’s next console, the Nintendo Switch, is set to arrive in March 2017. It’s a home console/portable console hybrid the idea is you can play the same games at home as you do on, say, the bus to work. It’s rumored to be nearly as powerful as the PlayStation 4 and Xbox One.

The gimmick of the Switch is its detachable screen. The screen itself is the console, processing and all it’s basically a tablet with a bunch of peripherals.

You attach the screen to two "Joy-Con" controllers and it becomes a portable console. Or you slide out the kickstand and use the controllers as gamepads, one in each hand. Or you slide the screen into a dock at home and it becomes a home console.

Or, apparently, you slide the screen into a VR headset and it becomes a full-on virtual reality head-mounted display:

That image comes from a recently published patent, which Nintendo filed back in June 2016. The patent seemingly details the tablet at the heart of Nintendo Switch: the way it connects to a home console dock, and the way it connects to the Joy-Con controllers to become a portable gamepad.

And then, in the final example images of how the device could work, a headset is shown with a Switch tablet being slid into it. The corresponding text is fascinating:

"Fig. 60 [the headset patent drawing] is a diagram showing an example HMD [head-mounted display] accessory to which the main unit can be attached. An HMD accessory to be described below as an example accessory can be used as a so-called HMD (head-mounted display) with the main unit attached thereto."

To quickly translate that jargon into English, the text description of the headset image directly identifies it as a VR headset (an "HMD") that can be used by slotting the Switch tablet into the front. For comparison, Samsung’s Gear VR works similarly: Your Galaxy phone becomes the device powering VR and the screen used to see it, through the lenses of a peripheral headset.

gear vr galaxy s7 The phone is attached to the front and enters a VR mode. The concept in Nintendo’s patent is very similar, albeit with a Switch tablet instead of a smartphone.

There’s a ton more text about the headset in the patent, from how it can detect movement using the sensors already built into the Switch tablet, to how the Joy-Con gamepads can be used as controllers for the headset, and how the headset has lenses built in that will widen images for VR use.

All that said, patents aren’t necessarily plans. Hardware companies like Apple and Nintendo publish patents regularly, and often those patents lead to nothing. It’s entirely possible that this is little more than an idea. If nothing else, it hints at a potential unannounced feature of the Switch everything else detailed in the patent has already been revealed as actual plans by Nintendo for the Switch.

A representative for Nintendo offered the following statement to Business Insider: "We have no comment regarding this patent matter."

=~=~=~=

PS4’s Battlezone Will Soon Look Like The 1980s Original With a Free Update

A free update is on the way for Battlezone that will let you play with its graphics similar to the the 1980 original.

Revealed through the trailer below, Classic mode is coming as part of a free update on December 20. The PlayStation VR game will allow you to take part in a "retro score-attack game set across the iconic black and green worlds of the original."

The original Battlezone, released by Atari in 1980, was technically in black and white, though a green overlay gave it the distinct look most players will recognize. What’s seen in the trailer seems to be a pretty faithful recreation of those graphics, albeit at a much higher fidelity.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

The Simple Email That Let Russia Hack the DNC

By now, U.S. intelligence agencies have established that Russia did in fact hack both the Democratic National Committee and the Republican National Committee, which ultimately lead to the leaking of information intended to swing the 2016 election in favor of Donald Trump. Now, new reporting from The New York Times has some horrifying details on exactly how Russian hackers were able to break into the systems, and they illustrate some important lessons we could all stand to learn.

According to The New York Times, the Russian cyberinvasion of the DNC’s servers took place in two stages, but the second and most severe breach happened in mid-March when Hillary Clinton’s campaign chairman John Podesta’s private email account was hacked after he clicked on a phishing email, a fake correspondence purportedly from Google but actually from hackers, one designed to trick the recipient into revealing a password.

The Times got a look at the same attack as directed at another Clinton campaign official, Billy Rinehart.

The attack referenced by the email is all but certainly fictitious, whereas the real attack is the big blue button, which does not actually lead to Google’s but instead to an attacker’s where all information will be intercepted. And as far as phishing emails go, it’s pretty good! There are no obvious misspellings or other blatant errors that might expose the ruse.

The full leaked emails from Wikileaks reveal two important details: the address the email came from, and the link the button pointed to. In the case of most phishing attacks, these are the most obvious points where a hacker's illusions slip. Unable to use an actual @google.com email address or official Google website, hackers can only opt for rough approximations. In this case, the email came from "no-reply@accounts.googlemail.com" and the link in the email was obscured by the link-shortening service Bit.ly.

What's worse is that, according to the report, one aide actually singled out the email as suspect, but another confirmed it to be legitimate, in what he now says was actually a typo. Per The Times:

"This is a legitimate email," Charles Delavan, a Clinton campaign aide, replied to another of Mr. Podesta's aides, who had noticed the alert. "John needs to change his password immediately. "With another click, a decade of emails that Mr. Podesta maintained in his Gmail account - a total of about 60,000 - were unlocked for the Russian hackers. Mr. Delavan, in an interview, said that his bad advice was a result of a typo: He knew this was a phishing attack, as the campaign was getting dozens of them. He said he had meant to type that it was an "illegitimate" email, an error that he said has plagued him ever since.

Changing the password is generally not a bad idea when you are worried someone may be attempting to attack your account, but it was the method by which it was done-clicking the big blue button - that was the grave error. If there's one bit of useful, personal advice to come out of this whole mess it is this: Never ever change your password using a link from an unsolicited in-bound email. Instead, go to the website directly to start the process there, and do it on another device if you want to be extra careful.

Chances are there is not an entire presidential election at stake in your case, but it's an important thing for all of us to learn.

Yahoo Says 1 Billion User Accounts Stolen in What Could Be Biggest Hack Ever

More than 1 billion Yahoo user accounts including phone numbers, birthdates, and security questions may have been stolen by hackers during an attack that took place in August 2013, the company revealed on Wednesday.

The announcement of what could represent the largest hack of all time is a separate incident than the one Yahoo disclosed back in September. In that hack, Yahoo said that at least 500 million user accounts were compromised.

"The company has not been able to identify the intrusion associated with this theft," Yahoo said on Wednesday about the

new incident.

News of the breach sent Yahoo shares sliding about 2.5% in after-hours trading on Wednesday.

The revelation of the hack could have implications for the $4.8 billion sale of Yahoo to Verizon, which has yet to close. Yahoo disclosed the previous hack to Verizon only after agreeing to the deal, and Verizon has since said that it considers the hack a material event that could affect the terms and price of the acquisition.

"As we ve said all along, we will evaluate the situation as Yahoo continues its investigation," Verizon told CNBC on Wednesday, regarding the latest hack.

Forged cookies

With a billion accounts at risk, that would make this the biggest breach of ever bigger than the Myspace breach of 360 million user accounts and 427 million passwords.

Yahoo said that payment-card data and bank-account information were not stored on the system the company "believes" was affected. But the hackers may have collected a trove of other valuable personal information, such as user names, email addresses, telephone numbers, dates of birth, hashed passwords, and, in some cases, encrypted or unencrypted security questions and answers.

Yahoo said that it now believes an "unauthorized third party accessed the company’s proprietary code to learn how to forge cookies." It was not clear which incident the forged cookies related to. But Yahoo said that "the company has connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft the company disclosed on September 22, 2016."

Here’s the entire message from Yahoo:

"Yahoo! Inc. has identified data security issues concerning certain Yahoo user accounts. Yahoo has taken steps to secure user accounts and is working closely with law enforcement.

"As Yahoo previously disclosed in November, law enforcement provided the company with data files that a third party claimed was Yahoo user data. The company analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data. Based on further analysis of this data by the forensic experts, Yahoo believes an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts. The company has not been able to identify the intrusion associated with this theft. Yahoo believes this incident is likely distinct from the incident the company disclosed on September 22, 2016.

"For potentially affected accounts, the stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. The investigation indicates that the stolen information

did not include passwords in clear text, payment card data, or bank account information. Payment card data and bank account information are not stored in the system the company believes was affected.

"Yahoo is notifying potentially affected users and has taken steps to secure their accounts, including requiring users to change their passwords. Yahoo has also invalidated unencrypted security questions and answers so that they cannot be used to access an account.

"Separately, Yahoo previously disclosed that its outside forensic experts were investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the ongoing investigation, the company believes an unauthorized third party accessed the company's proprietary code to learn how to forge cookies. The outside forensic experts have identified user accounts for which they believe forged cookies were taken or used. Yahoo is notifying the affected account holders, and has invalidated the forged cookies. The company has connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft the company disclosed on September 22, 2016.

"Yahoo encourages users to review all of their online accounts for suspicious activity and to change their passwords and security questions and answers for any other accounts on which they use the same or similar information used for their Yahoo account. The company further recommends that users avoid clicking links or downloading attachments from suspicious emails and that they be cautious of unsolicited communications that ask for personal information. Additionally, Yahoo recommends using Yahoo Account Key, a simple authentication tool that eliminates the need to use a password on Yahooaltogether.

Additional information is available on the Yahoo Account Security Issues FAQs page: https://yahoo.com/security-update.

Yahoo Suffers World's Biggest Hack Affecting 1 Billion Users

Yahoo has discovered a 3-year-old security breach that enabled a hacker to compromise more than 1 billion user accounts, breaking the company's own humiliating record for the biggest security breach in history.

The digital heist disclosed Wednesday occurred in August 2013, more than a year before a separate hack that Yahoo announced nearly three months ago . That breach affected at least 500 million users, which had been the most far-reaching hack until the latest revelation.

"It's shocking," security expert Avivah Litan of Gartner Inc.

Both lapses occurred during the reign of Yahoo CEO Marissa Mayer, a once-lauded leader who found herself unable to turn around the company in the four years since her arrival. Earlier this year, Yahoo agreed to sell its digital operations to Verizon

Communications for $4.8 billion a deal that may now be imperiled by the hacking revelations.

Yahoo didn’t say if it believes the same hacker might have pulled off two separate attacks. The Sunnyvale, California, company blamed the late 2014 attack on a hacker affiliated with an unidentified foreign government, but said it hasn’t been able to identify the source behind the 2013 intrusion.

Yahoo has more than a billion monthly active users, although some have multiple accounts and others have none at all. An unknown number of accounts were affected by both hacks.

In both attacks, the stolen information included names, email addresses, phone numbers, birthdates and security questions and answers. The company says it believes bank-account information and payment-card data were not affected.

But hackers also apparently stole passwords in both attacks. Technically, those passwords should be secure; Yahoo said they were scrambled twice once by encryption and once by another technique called hashing. But hackers have become adept at cracking secured passwords by assembling huge dictionaries of similarly scrambled phrases and matching them against stolen password databases.

That could mean trouble for any users who reused their Yahoo password for other online accounts. Yahoo is requiring users to change their passwords and invalidating security questions so they can’t be used to hack into accounts. (You may get a reprieve if you’ve changed your password and questions since September.)

Security experts said the 2013 attack was likely the work of a foreign government fishing for information about specific people. One big tell: It doesn’t appear that much personal data from Yahoo accounts has been posted for sale online, meaning the hack probably wasn’t the work of ordinary criminals.

That means most Yahoo users probably don’t have anything to worry about, said J.J. Thompson, CEO of Rook Security.

News of the additional hack further jeopardizes Yahoo’s plans to fall into Verizon’s arms. If the hacks cause a user backlash against Yahoo, the company’s services wouldn’t be as valuable to Verizon, raising the possibility that the sale price might be re-negotiated or the deal may be called off. The telecom giant wants Yahoo and its many users to help it build a digital ad business.

After the news of the first hack broke, Verizon said it would re-evaluate its Yahoo deal and in a Wednesday statement said it will review the "new development before reaching any final conclusions." Spokesman Bob Varettoni declined to answer further questions.

At the very least, the security lapses "definitely will help Verizon in its negotiations to lower the price," Litan predicted. Yahoo has argued that news of the 2014 hack didn’t negatively affect traffic to its services, strengthening its

contention that the Verizon deal should be completed under the original terms.

"This just adds to fuel to the fire and it won’t help Yahoo’s cause," said Eric Jackson, a longtime critic of the company’s management. Although he has in the past, Jackson doesn’t currently own Yahoo stock.

Investors appeared worried about the Verizon deal. Yahoo’s shares fell 96 cents, or 2 percent, to $39.95 after the disclosure of the latest hack.

Is Gmail More Secure Than Yahoo?

Yahoo confirmed 1 billion of its email accounts had been breached, but Gmail also has reported intrusions.

With Yahoo s announcement it had confirmed 1 billion of its accounts had been hacked, you may be wondering which email provider is the most secure.

Yahoo said Wednesday user data apparently was stolen by a state-sponsored actor in August 2013, including names, email addresses, telephone numbers, birth dates, passwords, and security questions and answers. It was the second confirmation of a massive intrusion in recent months. Yahoo announced Sept. 22 an intruder had used forged cookies to gain access to 500 million accounts.

But Yahoo is far from the only provider that has been hacked. Google announced last month it had patched a hole in its Gmail verification system that allowed a hacker to hijack a targeted Gmail account.

The hack exploited a verification bypass vulnerability that allows users to send email from a second Gmail account and make it look like the target account was the sender. The problem was discovered by security researcher Ahmed Mehtab, founder of Security Fuse.

Kaspersky Lab reported Mehtab was able to send email as google@gmail.com and gmail@gmail.com by using deactivated, nonexistent or blocked email accounts.

People running an older version of Android could be putting their Gmail accounts at risk, CheckPoint reported Nov. 30. The cybersecurity firm said a piece of malware called Gooligan mines Android devices for email addresses and authentication tokens, giving hackers the ability to breach Gmail, Google Photos, Google Docs, Google Play, Google Drive and G Suite accounts. The company said 1 million Google accounts had been affected at a rate of 13,000 devices a day.

WikiHow lists several ways to hack Gmail, admonishing that it s illegal to hack anyone s account except your own. The first method involves a key logger that needs to be installed on a target computer. The second method is to enable autofill and let

the computer do the work for you. The third method is to use a packet sniffer, which seeks out cookies.

There are three easy ways to determine if your Gmail account has been hacked, ShoutMeLoud advised last month. One way is to check the activity log at the bottom of your account page to determine when the account was last accessed. The second is to go to the forwarding page and determine whether someone has been rifling your account. Also check to see if the IMAP and/or POP features are enabled. If they are and you re not using a third-party email program, turn them off since anyone can collect your email in their accounts if they know your password.

Facebook Users Are Fed Up With Fake News

Each week day after making the kids' lunches, Lisel Laslie takes out her iPhone to scroll through Facebook over her morning cup of coffee.

At noontime, while eating lunch at her desk, this 48-year-old mother of two from Tallahassee, Fla., sneaks another peek at her notifications and News Feed. In the evening after she tucks the kids into bed, she curls up in the living room for an hour or two of blissfully uninterrupted social-media updates.

But, over the summer when bogus articles trashing both presidential candidates began flooding her News Feed, Laslie began posting less frequently and spending less time on Facebook.

"Facebook is a place to go for distraction. I want to see puppies and pictures of my friends' kids. Then your feed gets clogged up with all that stuff," she said.

Facebook has a fake news problem. And some of its users are fed up with it. They're not sure if the solution is to let the social network, with its own biases, decide what's true. Or whether they themselves should become better fact-checkers.

"I find myself wasting my day verifying stories," says Kristen Stanley, a 49-year-old homemaker from Morgan City, LA, who used to work in the ship building industry. "I didn't used to do that. It's all new and it's all started with the election."

It turns out that by creating the world's most popular place to share, Facebook also created the world's most efficient delivery system for fake news.

Some 170 million people in North America use Facebook every day. Nearly half of all adults in the U.S. say they get their news from Facebook. Fake news creates significant public confusion about current events, with nearly one-fourth of Americans saying they have shared a fake news story, according to a Pew Research Center survey.

And that ticks off Stanley. She wishes her friends would do some research before sharing "nonsense."

"Some of it makes me wonder if my friends have brains," says Stanley, whose News Feed during the election was rife with "things on both sides that were completely false."

Facebook has taken a lot of heat since the election for not doing enough to remove fake news reports, such as a widely shared but erroneous article claiming Pope Francis endorsed Donald Trump.

The giant social network is taking steps to do something about it. On Thursday Facebook said it was rolling out a series of experiments to stem the flow of fake news. It plans to make it easier to report a hoax and for fact-checking organizations to flag fake articles. It's also removing financial incentives for spammers and plans to pay closer attention to other signals, such as which articles Facebook users read but then don't share. Last month, Facebook barred fake news sites from using its ad-selling services.

Not everyone is happy about that. When Facebook CEO Mark Zuckerberg announced efforts to wipe out fake news in a Facebook post, some users responded with skepticism.

"How will you know if these fact checkers are not politically motivated or affiliated themselves?" one user asked. "Even 'respected' news outlets are biased and misrepresent news as it is. It's a very grey complex area."

Another replied: "People choose what they want to read and what they don't want to read, so what gives you the right to decide what people get to read?"

Stanley, a Trump supporter, says demonstrably false news needs to go.

"I really do believe these articles cause problems. They destroy friendships," she said. "Facebook people take it way too seriously and extremely personally. Everything is so negative now. I don't like to get on Facebook. It's depressing."

Sharing fake news has picked fights and eroded family ties. Summer Davis, 35, a writer and blogger from Santa Rosa Beach, Fla., says she has family members who regularly spread fake news. She even unfollowed one of them whom she says scans headlines of fake news articles and shares them without reading them, the more sensational the better.

Davis says she herself hasn't been fooled by fake news. But, she says, "some of the headlines have definitely caused some anxiety before I could fact-check."

Holding Facebook responsible for the fake-news onslaught doesn't sit right with Davis, though. That, she says, "is like blaming McDonald's for obesity."

"The real problems are ignorance and this fast-food society that expects information served hot and fast whether it's true or not," she said. "There is too much knee-jerk emotion happening and not enough fact checking."

Conservative concern: censorship

Not everyone wants Facebook to step in and become the arbiters of what content is misleading. That is rooted in the growing distrust of establishment news sources. A Gallup poll in September said Americans' trust in the media had sunk to its lowest point ever, with only 32% of American saying they have a "great deal" or "a fair amount" of confidence that the media reports the news "fully, accurately and fairly."

Danielle Sgantas, a self-identified conservative from Yucca Valley, Calif., says she has never been fooled by fake news sites. And, she says, she believes the fake news controversy was created to crack down on alternative sources of news "so that we only get the news that the Democrats, which includes about 99% of the news media, wants us to hear and believe."

"I want freedom of speech to continue. I want alternative news sites not to be censored," she said. "I can determine what is real and what is not real by making searches on my own."

Others believe something has to be done. Whitney Hoffman, a 50-year-old digital marketer from Chadds Ford, Pa., says fake news is a virus that should be stamped out by any means necessary. Every day during the election, she says she saw things in her News Feed "that were completely false and that were obviously false." But, she says, she also saw fake news that could dupe even very news savvy people.

"Some of it sounds plausible and when it's spread by trusted friends, there's an assumption it must be true," Hoffman said. "I feel like we all need to wear finger condoms every day otherwise we are going to spread fake-news viruses everywhere."

Laslie, who says she was embarrassed when she unwittingly shared fake news on Facebook, has come up with a radical solution of her own. She doesn't share articles on Facebook anymore. It's just too much work figuring out what's real, she says.

"It's like I am an investigative reporter and I have to check eight sources before sharing anything," Laslie said. "I will share pictures of kitties and animals all day long before I share a news story."

Facebook Is Going To Use Snopes and Other Fact-checkers To Combat and Bury 'Fake News'

Facebook is going to start fact-checking, labeling, and burying fake news and hoaxes in its News Feed, the company said Thursday.

The decision comes after Facebook received heated criticism for its role in spreading a deluge of political misinformation during the US presidential election, like one story that falsely said the Pope had endorsed Donald Trump.

To combat fake news, Facebook has teamed up with a shortlist of media organizations, including Snopes and ABC News, that are part

of an international fact-checking network led by Poynter, a nonprofit school for journalism in St. Petersburg, Florida.

Starting as a test with a small percentage of its users in the US, Facebook will make it easier to report news stories that are fake or misleading. Once third-party fact-checkers have confirmed that the story is fake, it will be labeled as such and demoted in the News Feed.

A company representative told Business Insider that the social network will also use other signals, like algorithms that detect whether a story that appears fake is going viral, to determine if it should label the story as fake and bury it in people’s feeds.

"We’ve focused our efforts on the worst of the worst, on the clear hoaxes spread by spammers for their own gain, and on engaging both our community and third party organizations," Facebook News Feed chief Adam Mosseri said in a company blog post on Thursday.

A team of Facebook researchers will also review website domains and send sites that appear to be fake or spoofed (like "washingtonpost.co") to third-party fact-checkers, a Facebook representative said. Of the 42 news organizations that have committed to Poynter’s fact-checking code of ethics, Facebook is starting out with the following four: Snopes, Factcheck.org, ABC News, and PolitiFact.

The Associated Press will also be a fact-checking partner.

"We are only involved to the extent that Facebook relies on the list of signatories to our code of principles as a starting point for the organizations it chooses to verify," a Poynter representative told Business Insider. "Facebook is the only organization certifying third party fact-checkers on its platform."

Facebook has given its four initial fact-checking partners access to a tool that will let them label stories in the News Feed as fake, a Facebook spokesperson said. The person said Facebook is not paying the organizations to fact-check.

The websites that Facebook determines to be fake news organizations or spoofed domains will also not be able to sell ads on the social network. Owners of fake-news sites can make thousands of dollars per month through internet ads.

Facebook has repeatedly said that it’s not a media company, but rather an open technology platform that relies on media publishers and its users to share accurate information.

We do not think of ourselves as editors," Patrick Walker, Facebook’s head of media partnerships, said during a recent journalism conference in Dublin. "We believe it s essential that Facebook stay out of the business of deciding what issues the world should read about. That s what editors do.

Politicians such as President Barack Obama and former Secretary of State Hillary Clinton have recently expressed concern about the prevalence of misinformation on social media, with Obama

calling it a "dust cloud of nonsense" and Clinton calling it "an epidemic."

Facebook CEO Mark Zuckerberg has meanwhile gone so far as to say that it’s "pretty crazy" for some to suggest that fake news on Facebook could have swayed the election in favor of either candidate.

But after facing significant backlash for its denial to fact-check stories on its network, Zuckerberg now calls Facebook a "new kind of platform" with a responsibility to "build a space where people can be informed."

"Facebook is a new kind of platform different from anything before it. I think of Facebook as a technology company, but I recognize we have a greater responsibility than just building technology that information flows through," the Facebook founder said in a Thursday post.

"While we don’t write the news stories you read and share, we also recognize we’re more than just a distributor of news. We’re a new kind of platform for public discourse and that means we have a new kind of responsibility to enable people to have the most meaningful conversations, and to build a space where people can be informed."

You can read Zuckerberg’s full post below:

A few weeks ago, I outlined some projects we’re working on to build a more informed community and fight misinformation. Today, I want to share an update on work we’re starting to roll out.

We have a responsibility to make sure Facebook has the greatest positive impact on the world. This update is just one of many steps forward, and there will be more work beyond this.

Facebook is a new kind of platform different from anything before it. I think of Facebook as a technology company, but I recognize we have a greater responsibility than just building technology that information flows through. While we don’t write the news stories you read and share, we also recognize we’re more than just a distributor of news. We’re a new kind of platform for public discourse -- and that means we have a new kind of responsibility to enable people to have the most meaningful conversations, and to build a space where people can be informed.

With any changes we make, we must fight to give all people a voice and resist the path of becoming arbiters of truth ourselves. I believe we can build a more informed community and uphold these principles.

Here’s what we’re doing:

Today we’re making it easier to report hoaxes, and if many people report a story, then we’ll send it to third-party fact checking organizations. If the fact checkers agree a story is a hoax, you’ll see a flag on the story saying it has been disputed, and that story may be less likely to show up in News Feed. You’ll still be able to read and share the story, but you’ll now have

more information about whether fact checkers believe it’s accurate. No one will be able to make a disputed story into an ad or promote it on our platform.

We’ve also found that if people who read an article are significantly less likely to share it than people who just read the headline, that may be a sign it’s misleading. We’re going to start incorporating this signal into News Feed ranking.

These steps will help make spreading misinformation less profitable for spammers who make money by getting more people to visit their sites. And we’re also going to crack down on spammers who masquerade as well-known news organizations.

You can read more about all of these updates here: http://newsroom.fb.com/?p=7014

This is just one of many steps we’ll make to keep improving the quality of our service. Thanks to everyone for your feedback on this, and check back here for more updates to come.

Facebook Lets Users Click To Report Fake News

Facebook announced Thursday it was offering a tool allowing users to report fake news, a move aimed at stemming a wave of misinformation which some claim influenced the 2016 US election.

"We believe in giving people a voice and that we cannot become arbiters of truth ourselves, so we’re approaching this problem carefully," Facebook’s vice president Adam Mosseri said in a blog post.

"We’ve focused our efforts on the worst of the worst, on the clear hoaxes spread by spammers for their own gain, and on engaging both our community and third-party organizations."

Facebook said it would begin testing a system allowing users to click on a news item if they suspect it is fabrication.

The huge social network said it would work with global fact-checking organizations subscribing to the Poynter Institute’s International Fact Checking Code of Principles.

"If the fact-checking organizations identify a story as fake, it will get flagged as disputed and there will be a link to the corresponding article explaining why," Mosseri said. "Stories that have been disputed may also appear lower in News Feed."

Facebook has been under fire for failing to stem a wave of fake news, which according to some critics may have helped the election of Republican property tycoon Donald Trump by spreading unfounded negative news about his Democratic opponent Hillary Clinton.

Facebook has dismissed the notion that fake news shared on the social network swung the election results but has been stepping up its efforts to weed out clearly false news.

The US social giant, with some 1.8 billion users worldwide, has however avoided being labeled a "media company" or implemented efforts to impose editorial judgments on news being shared.

Separately Thursday, a survey by the Pew Research Center showed nearly two out of three US adults (64 percent) believed fake news causes confusion about basic facts in current events.

Although many respondents said they sense fake stories are spreading confusion, they were relatively confident in their own ability to detect hoaxes.

The survey found 39 percent "very confident" that they can recognize news that is fabricated and another 45 percent "somewhat confident."

However, nearly one in four said they have shared a made-up news story: 14 percent acknowledged they shared a news item they knew was fake at the time and 16 percent saying they shared a story they later realized was fake.

Concerns over fake news grew during the 2016 presidential campaign amid widespread sharing of hoaxes including stories saying Pope Francis had endorsed Donald Trump, or that Hillary Clinton was linked to a pedophilia ring operating out of a pizzeria.

The survey of 1,002 adults was conducted December 1-4, with the margin of error estimated at 3.6 percentage points.

U.S. Charges Nigerian with Role in Cyber Scam Targeting Thousands

A Nigerian man is facing U.S. charges that he participated in scams targeting thousands of victims globally in which company executives or vendors were impersonated in emails directing employees to make large wire transfers.

David Chukwuneke Adindu, 29, pleaded not guilty in Manhattan federal court on Wednesday to charges including wire fraud, prosecutors said, more than three weeks after the FBI said he was arrested at a Houston airport.

Adindu’s attorney could not be immediately identified.

The case was the latest example of a growing type of cyber scam called a "business email compromise," in which fraudsters target businesses that work with foreign suppliers or regularly perform wire transfers.

The Federal Bureau of Investigation said in June that since October 2013, U.S. and foreign victims have reported 22,143 complaints involving business email compromise scams in which criminals sent requests for almost $3.1 billion in transfers.

According to the indictment, Adindu, who during the period in question resided in both Guangzhou, China and Lagos, Nigeria,

worked with others to carry out the scams from 2014 to 2016.

The indictment said Adindu and others exchanged information regarding, among other things, scripts for requesting wire transfers and lists of names and email addresses for contacting and impersonating potential victims.

Among those targeted, the indictment said, was an unnamed New York investment firm, where an employee received an email claiming in June 2015 to be from an investment adviser at another firm asking for a $25,200 wire transfer.

The employee later learned the email was not actually sent by that adviser, and as a result did not comply with a second wire transfer request for $75,100, the indictment said.

The case is U.S. v. Adindu, U.S. District Court, Southern District of New York, No. 16-cr-00575.

Man Who Hacked 130 Celebrities Jailed for Five Years

Maybe you ll recall 24-year-old Bahamian Alonzo Knowles, who recently pleaded guilty to hacking the email accounts of some 130 media, sports and entertainment celebrities? And trying to sell everything from their confidential scripts to their sex tapes? The judge just threw the book at him: five years in federal prison.

That s roughly twice the 27 to 33 months you might have expected from the US federal sentencing guidelines, according to the New York Times. Why such a tough sentence? Because Knowles made a couple of really dumb mistakes.

Dumb mistake #1: flying to New York to sell a stolen script to a Department of Homeland Security undercover agent, and telling the fully-wired agent all about how he d done it all.

As the NYT reported when Knowles was arrested:

> He gave an interested buyer his name, birth date, passport number and money transfer account number to set up the trip Mr. Knowles told [the undercover agent] that going after a high-profile celebrity can be difficult.
>
> So, instead, he used what he described as his social engineering process, in which he identified celebrities friends through photos and got into the friends email accounts to learn about his target

Dumb mistake #2: given access to a prison email system the authorities told him they monitored, Knowles wrote:

> When i get out im gon shake up hollywood for real!

..and (promising to write a book about the stars he d hacked):

> Im name dropping everyone involved and what i know and im

including pictures of paperwork that aint public.

and:

This gonna be the most talked about thing on tv Eat a steak for me tomorrow.

and, to a female friend:

These people dont want me to be a millionaire. They want me be a loser and not be able to afford women like you lol.

and, last but not least:

Everyone loves gossip. I cant wait to get out i already know how the cover is gonna look.

The prosecutor and judge were not impressed with his lawyer s claim that Knowles was just a lonely guy, trying to impress a woman. Hence five full years in a federal penitentiary.

This is more than another incompetent criminal story: Knowles s very human victims deserve to be heard.

Fortunately, one of them Naturi Naughton (pictured), an actor on the Starz network show Power recorded an eloquent victim statement. We thought it was worth quoting at length:

I felt violated. This man hacked into my personal emails, my account, jeopardized my job by potentially trying to sell scripts to my show Power, he stole six of those scripts and tried to extort me, my producer 50 Cent, and my showrunner. I know a lot of public figures and celebrities go through this, so the only reason I wanted to talk about this was, I m sick of it, people in the public eye being treated like we can just be hacked into and [steal] naked pictures, our information he had all my passwords, [jeopardized] my financial stability

It s really a frustrating and emotional experience, because I couldn t control it. While I was being hacked I noticed my email passwords were constantly being changed, and then my boss at Starz called about the scripts being basically stolen, I had never felt more violated and out of control in my entire life.

I never thought I would be a victim of this kind of cybercrime. But it s serious, and I hope the man who did this thinks about how he affected not just me but so many other people s lives, who worked really hard. We don t deserve it. This can t be acceptable. It s not a game, it s not a joke, this is our lives I would never wish this on anyone.

Seconded.

U.S. Indicts Three Romanians Over $4 Million Cyber Fraud

Three Romanian nationals have been extradited to the United States to face charges that they operated a cyber fraud scheme

in which they infected at least 60,000 computers and stole at least $4 million, U.S. prosecutors said on Friday.

Bogdan Nicolescu, 34, Tiberiu Danet, 31, and Radu Miclaus, 34, were charged in an indictment filed in federal court in Cleveland with charges including wire fraud, aggravated identity theft and conspiracy to commit money laundering.

The trio were extradited to the United States this week after being arrested in Romania earlier this year, prosecutors said. In court on Friday, Danet and Miclaus pleaded not guilty. Nicolescu has not yet been arraigned, court records show.

Danet’s lawyer confirmed his client pleaded not guilty. A lawyer for Miclaus did not respond to requests for comment and an attorney for Nicolescu could not be identified.

Prosecutors said they belonged to a group in Bucharest called "Bayrob" that in 2007 began to develop and deploy malware sent through emails claiming to be from entities like Western Union, Norton AntiVirus and the U.S. Internal Revenue Service.

Prosecutors said after users clicked on an attached file, the malware would get installed on the computer. It would then harvest email addresses from contact lists or email accounts, which then received email with the malware as well, they said.

More than 60,000 computers were infected, prosecutors said. Once infected, the defendants could control these computers to collect information including credit card details, user names and passwords, they said.

They also used the infected computers to mine for digital currencies like bitcoin, causing the devices to become unusable or slow, prosecutors said.

When users with infected computers visited websites like Facebook or eBay, the defendants would redirect the computer to a nearly identical site, allowing them to steal account credentials, prosecuotrs said.

They also placed over 1,000 listings for cars, motorcycles and other goods on auction sites like eBay with photos infected with malware that would redirect a victim who clicked on the image to fake webpages, prosecutors said.

These webpages prompted users to pay through a nonexistent "escrow agent" who wired the money to others in Eastern Europe, who then gave it to the defendants, prosecutors said, resulting in about $4 million in losses.

Symantec Corp, which in a statement claimed credit for helping unearth the "Bayrob" gang, said the group had stolen up to $35 million USD from victims through various means.

The case is U.S. v. Nicolescu et al, U.S. District Court, Northern District of Ohio, No. 16-cr-00224.

New Popcorn Time Malware Offers Victims Free Ransomware Decryption If They Help Infect Others

A new type of ransomware dubbed Popcorn Time was recently discovered by security researchers and brings with it a sinister twist that feels like some kind of strange psychological experiment.

Ransomware is a popular kind of malware attackers will use to infect a victim s computer. Once installed, the malware encrypts and, in some cases, locks files and data stored on the victim s computer or infected device. Attackers then demand a ransom payment in order to restore the files. For most ransomware infections, there is no way to decrypt scrambled files unless the victim purchases the decryption keys. If victims lack appropriate backups, they can find themselves shelling out hundreds or even thousands of dollars to have their files restored.

While most ransomware tends to work in the same way, cybercriminals are constantly coming up with new and more effective ways to wield their nasty tools. The latest Popcorn Time malware is no exception. First discovered by researchers on the MalwareHunterTeam, the Popcorn Time ransomware offers infected victims two choices for restoring their files one of which will challenge their moral fiber. Victims are given the option to pay the fee to decrypt their files or help the ransomware attackers spread the infection to others.

In the ransom message, Popcorn Time developers offer the nasty option of sharing a link to the Popcorn Time malware with people they know via email, text, etc. If two or more people end up getting infected by the link and pay the ransom, the attacker will give the original victim the gift of free encryption keys.

While I d really like to hope that no one would be desperate (or amoral) enough to actually share the Popcorn Time malware link with others, it definitely makes for an interesting study of moral scruples. The Popcorn Time malware is still only in development and hasn t actually been used in the wild yet, but it s nonetheless a concerning one to keep an eye on.

Ransomware has become one of the most widespread forms of malware used by cyber criminals and has taken a wide variety of victims captive from small businesses to major health care organizations. Just last month, ransomware attackers caused several networked computers on the San Francisco Public Transport System to be shut down, which lead to one day in which all passengers rode the MUNI light-rail system for free while the agency investigated the issue.

=~=~=~=